The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

06/14/2011

SUBJECT:

Vulnerability in Vector Markup Language (VML) Could Allow Remote Code Execution (MS11-052)

OVERVIEW:

A vulnerability has been discovered within Microsoft's web browser, Internet Explorer, that could allow for remote code execution. Specifically, the vulnerability is in the way Vector Markup Language (VML) is processed by Internet Explorer. VML is an XML-based language used to produce and render vector graphics. Successful exploitation could result in an attacker gaining the save privileges of the logged-on user. Depending on the privileges associated with the affected user, an attacker could then install programs, view, change, or delete data; or create accounts with full user rights.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered within Microsoft's Internet Explorer web browser that could allow for remote code execution within the context of the currently logged in user, potentially allowing for full control of a given system. This vulnerability lies within the way Internet Explorer accesses a VML object that has not been correctly initialized or has been deleted, which may corrupt memory in such a manner that could allow an attack to execute arbitrary code within the privileges of the logged-on user.

Vector Markup Language is an XML-based language used to produce and render vector graphics akin to canvas-based graphic suites. Even though VML use has decreased with the advent of SVG, it is still supported within Internet Explorer.

Exploitation of this vulnerability is possible if a user visits or is directed to a website delivering a specially crafted webpage. Additionally, an attacker could send a user a specially crafted Microsoft Office document that hosts the IE-rendering engine. Successful exploitation could result in an attacker gaining the save privileges of the logged-on user. Depending on the privileges associated with the affected user, an attacker could then install programs, view, change, or delete data; or create accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft immediately after appropriate testing.
- Read all e-mails in plain text.
- Run all software as a non-privileged user to diminish the effects of attack.
- Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones.
- Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/ms11-052.mspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1266

SecurityFocus:
http://www.securityfocus.com/bid/48173